KPMG

# KPMG Global Banking (APP) Scam Survey

## Strategies to manage authorized push payment fraud

27 June 2025

# Agenda

- Welcome and opening remarks
- Global Banking (APP) Scam Survey insights
    - Key findings from the survey
    - How banks are detecting, preventing, and responding to APP scams
    - Proactive measures to protect your bank's reputation
- Questions and answers

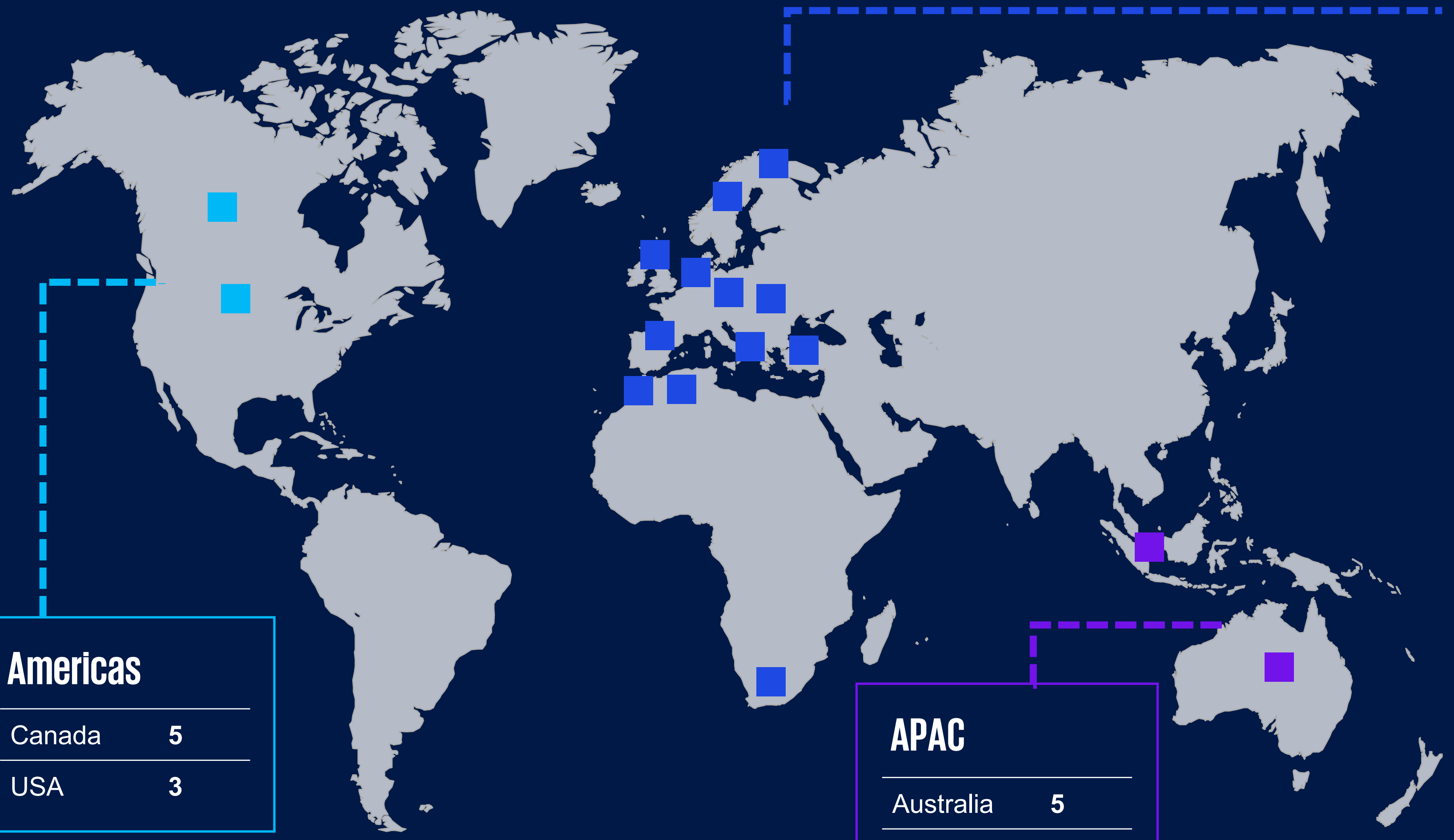
# Key insights
# from the APP Scam survey

# Coverage of our Global Banking (APP) Scam Survey

**48**
Banks

**16**
Countries

**5**
Continents



## Americas

| | |
|---|---|
| Canada | 5 |
| USA | 3 |

## APAC

| | |
|---|---|
| Australia | 5 |
| Singapore | 4 |

## EMEA

| | |
|---|---|
| Germany | 1 |
| Greece | 3 |
| Italy | 1 |
| Netherlands | 3 |
| Norway | 3 |
| Portugal | 2 |
| Spain | 2 |
| South Africa | 3 |
| Sweden | 3 |
| Switzerland | 1 |
| Türkiye | 2 |
| UK | 7 |

# Key insights

**E-commerce scams**

Largest volume

**Investment scams**

Largest financial impact

45% of surveyed banks consider off-boarding repeat scam victims as a last resort

Specialist teams review scam control measures within organizations.

Pausing/blocking transactions and sharing data with law enforcement were rated as the most effective prevention/detection.

Continuing education is needed across multiple platforms.

Patterns for APP scams are consistent at a global level.

**2 in every 5 respondents** do not have a technology stack with orchestration layers integrating a multitude of data sources into a single system

**60%** of respondents reported an increase in scam-related customer complaints

- dissatisfaction with reimbursement decisions,
- transaction friction,
- slow resolution speeds, and
- perceived insufficient consumer protection by banks

# Global Authorized Push Payment (APP) Scam Landscape

**E-commerce and purchase scams**
**(Largest in volume)**

**Investment scams**
(fake deposit, boiler room, fake cryptocurrency)
**(Largest by financial impact)**

**Sophisticated impersonation scams**
(CEO, bank employees, workplace, people of authority, tech support, accountants, phishing/quishing/ smishing/ vishing)

**Romance scams**

**Advance fee and payment scams**

**Business email compromise**

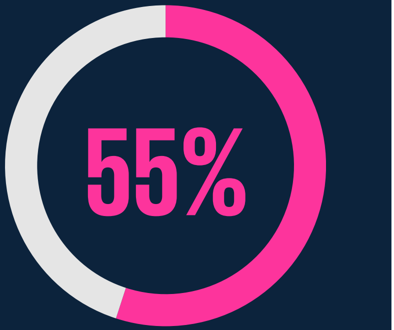
**Blurring and hybrid scams**

**Deepfakes**

**Me-to-me payments**

# APP Scam in Thailand

# The state of scams in Thailand 2024



of Thai respondents are confident in their ability to recognize scams.

89%

of Thai encounter scams at least once per month.

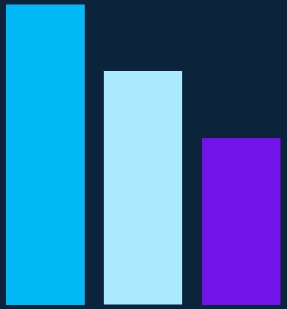
More than 1 in 4 respondents lost money in a scam in the past year.

Identity theft has overtaken shopping scams as the most prevalent type of fraud in Thailand.

On average, Thai victims

lost USD 1,106 each

contributing to a total loss of US$17.2 billion (or THB591.71 billion, equal to 3.4% of GDP).

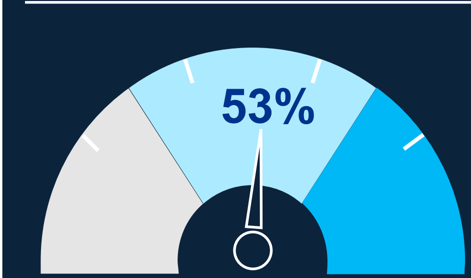


Majority of scams are delivered via phone calls or text/ SMS messages

**Thailand** remains one of the most active fertile ground for scammers and attempted scamming activities in this region.

86% of scam payments in Thailand are made through electronic/ bank transfer.

The remaining 14% of scam payments are spread relatively evenly across other payment methods: cash, peer-to-peer online payment, credit card, etc.



of scams are completed within 24 hours of first contact

**Facebook, LINE, Messenger** are the most exploited platforms.

**TikTok and Gmail** round out the top five platforms where people encounter scams.

*Source: The State of Scams in Thailand 2024, Global Anti-Scam Alliance (GASA)*

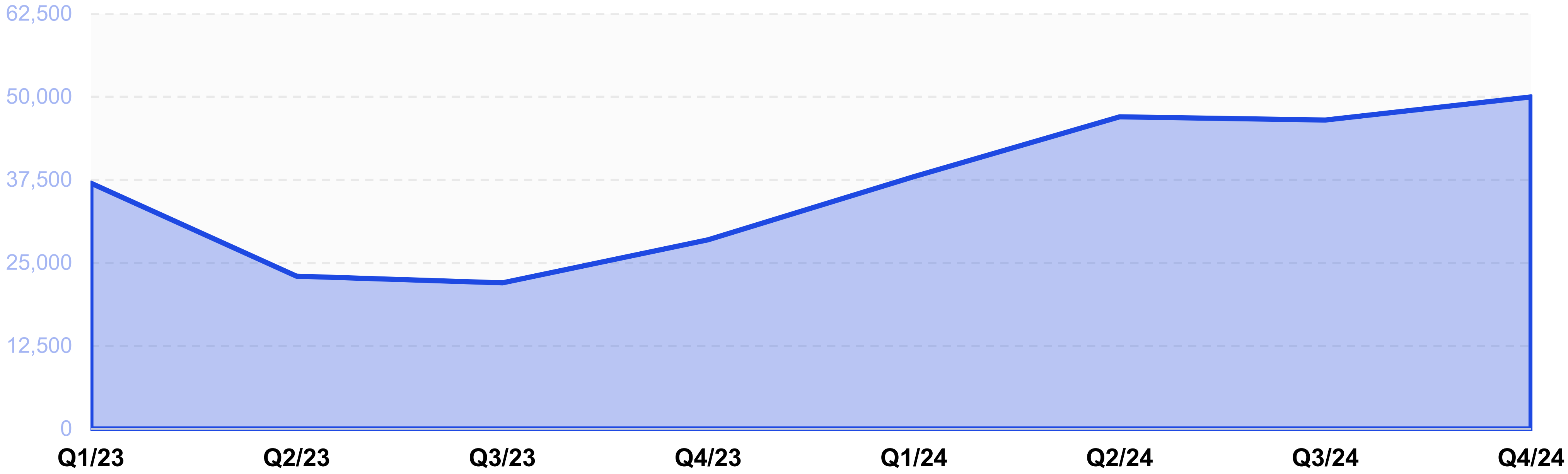
# Authorized Push Payment (APP) scams in Thailand

หลอกกู้ออนไลน์

Call center หลอกโอนเงิน

หลอกให้รัก

จำนวนเคส Purchase scam & Authorized Push Payment fraud



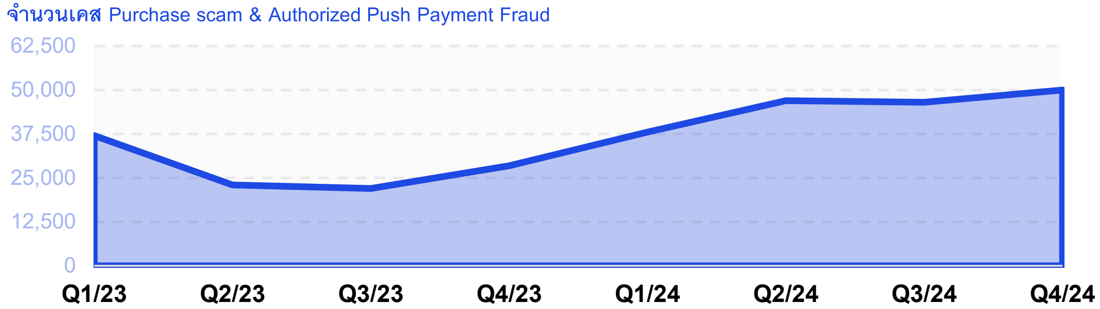
*ที่มา: คอลัมน์แจงสี่เบี้ย, ธนาคารแห่งประเทศไทย พฤษภาคม 2568*

# Authorized Push Payment (APP) scams in Thailand

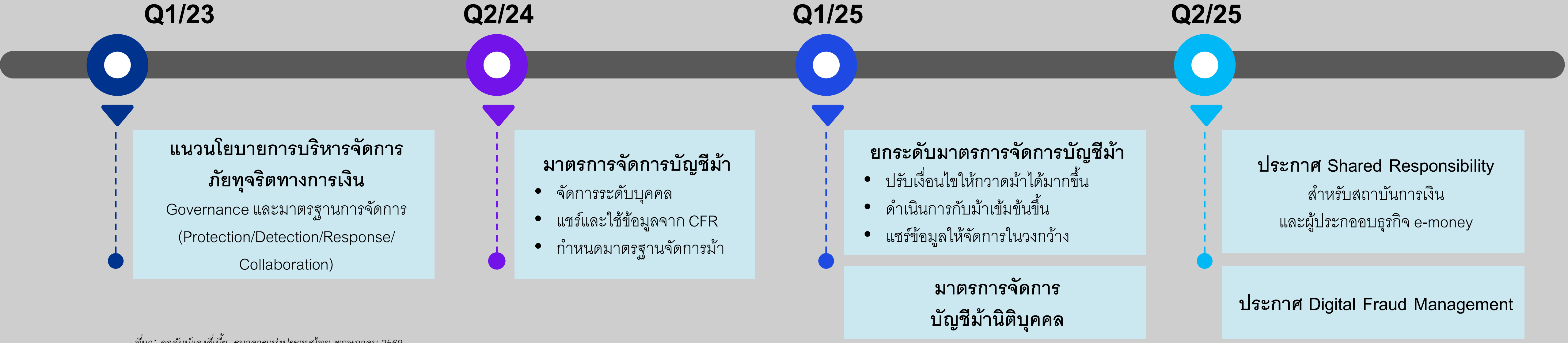
หลอกกู้ออนไลน์

Call center
หลอกโอนเงิน

หลอกให้รัก



## ธนาคารแห่งประเทศไทยกับการจัดการภัยทุจริตทางการเงิน



**แนวนโยบายการบริหารจัดการภัยทุจริตทางการเงิน**

Governance และมาตรฐานการจัดการ (Protection/Detection/Response/ Collaboration)

**มาตรการจัดการบัญชีม้า**

- จัดการระดับบุคคล
- แชร์และใช้ข้อมูลจาก CFR
- กำหนดมาตรฐานจัดการม้า

**ยกระดับมาตรการจัดการบัญชีม้า**

- ปรับเงื่อนไขให้กวาดม้าได้มากขึ้น
- ดำเนินการกับม้าเข้มข้นขึ้น
- แชร์ข้อมูลให้จัดการในวงกว้าง

**มาตรการจัดการบัญชีม้านิติบุคคล**

ประกาศ Shared Responsibility
สำหรับสถาบันการเงิน
และผู้ประกอบธุรกิจ e-money

ประกาศ Digital Fraud Management

*ที่มา: คอลัมน์แจงสี่เบี้ย, ธนาคารแห่งประเทศไทย พฤษภาคม 2568*

# How banks are detecting, preventing, and responding to APP scams

# Governance

## Scam strategies

- About half of the respondents already have or are working towards a dedicated scams policy.
- The others direct their efforts through integrated fraud prevention frameworks, with scam strategies commonly embedded within these initiatives.

# Governance

## Risk assessments

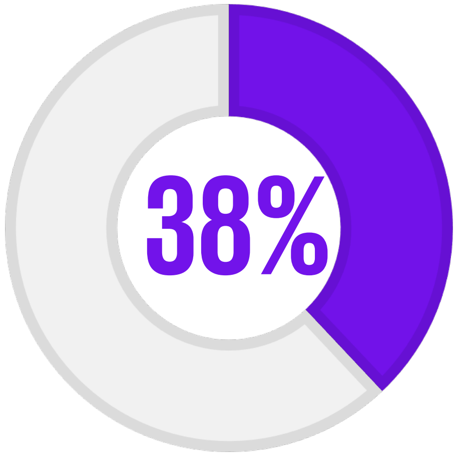
- 75% of respondents confirmed that they performed a risk assessment for APP scams, with some of these assessments included in product or fraud risk assessments.

## Management reporting

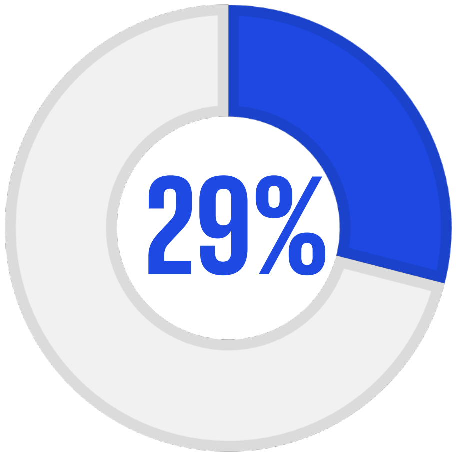
- A majority of banks surveyed (90%) acknowledge the importance of tracking customer scam losses separately from fraud losses.

# How do banks make sure their APP scam strategy is responsive to new scam typologies?

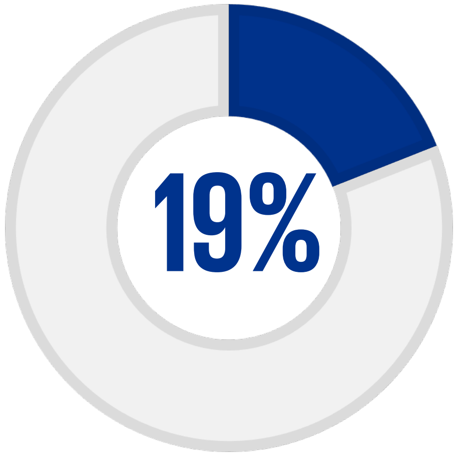
# How banks make sure their APP scam strategy is responsive to new scam typologies:



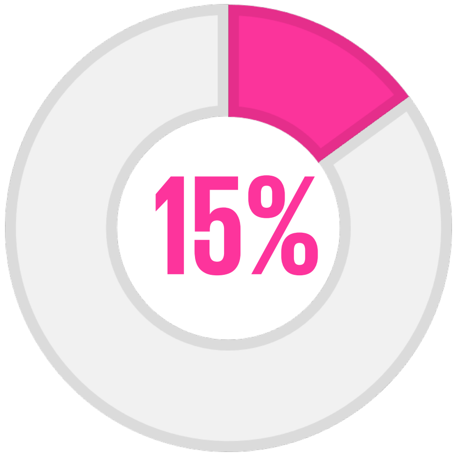
**Collaboration and information sharing** internally and externally



**Regular reviews** of their fraud control measures, incorporating global insights, and customer feedback



**Specialized teams and committees** are dedicated to evaluate current fraud cases, strategize and implement responsive actions

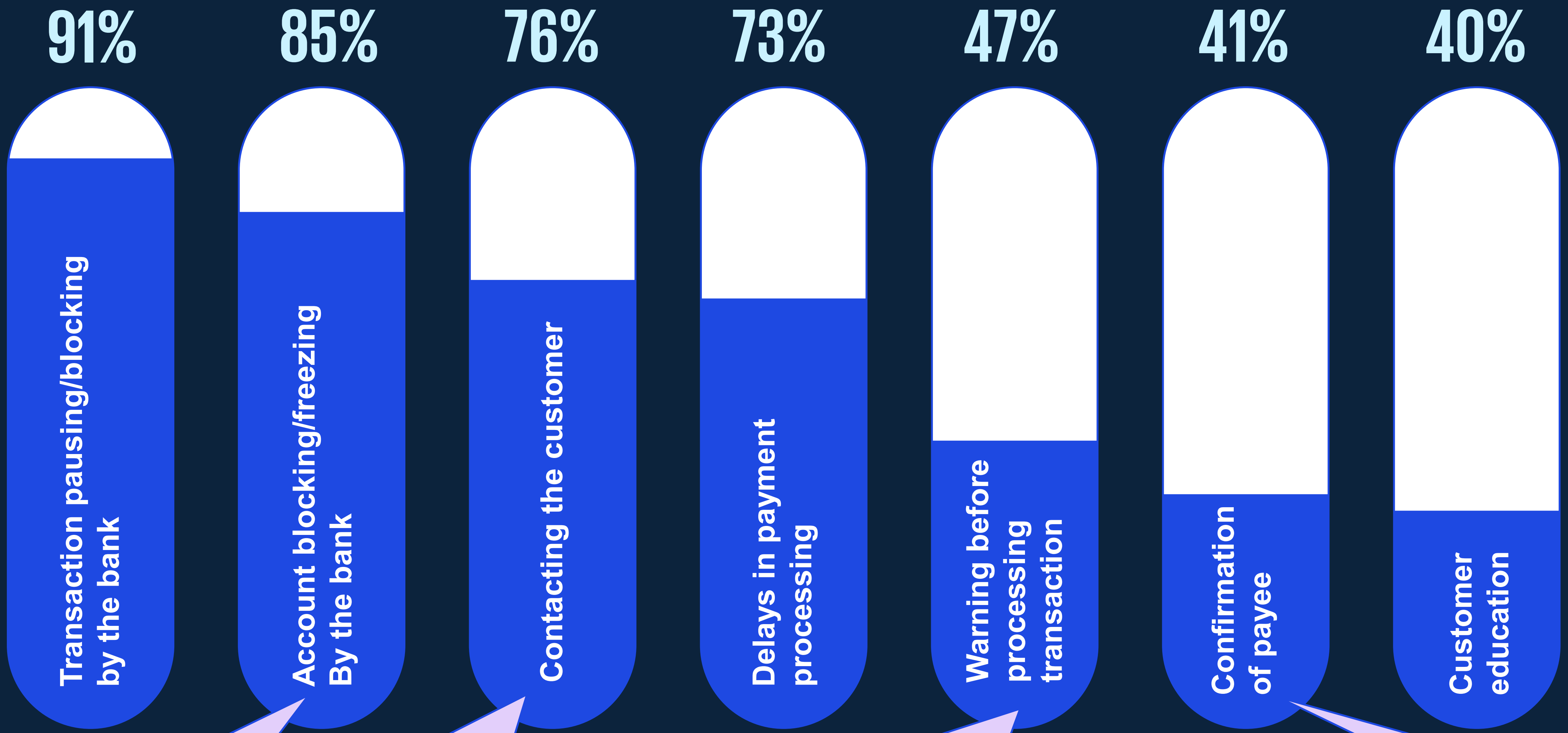


**Data-driven approaches** are applied to quickly identify and respond to emerging scam trends

# Prevention and detection

The strategies and controls implemented to protect individuals/organizations from scams and to identify fraudulent activities

# Effectiveness of prevention measures



Negative impact on genuine victims

Balance between invasion of privacy and money protection

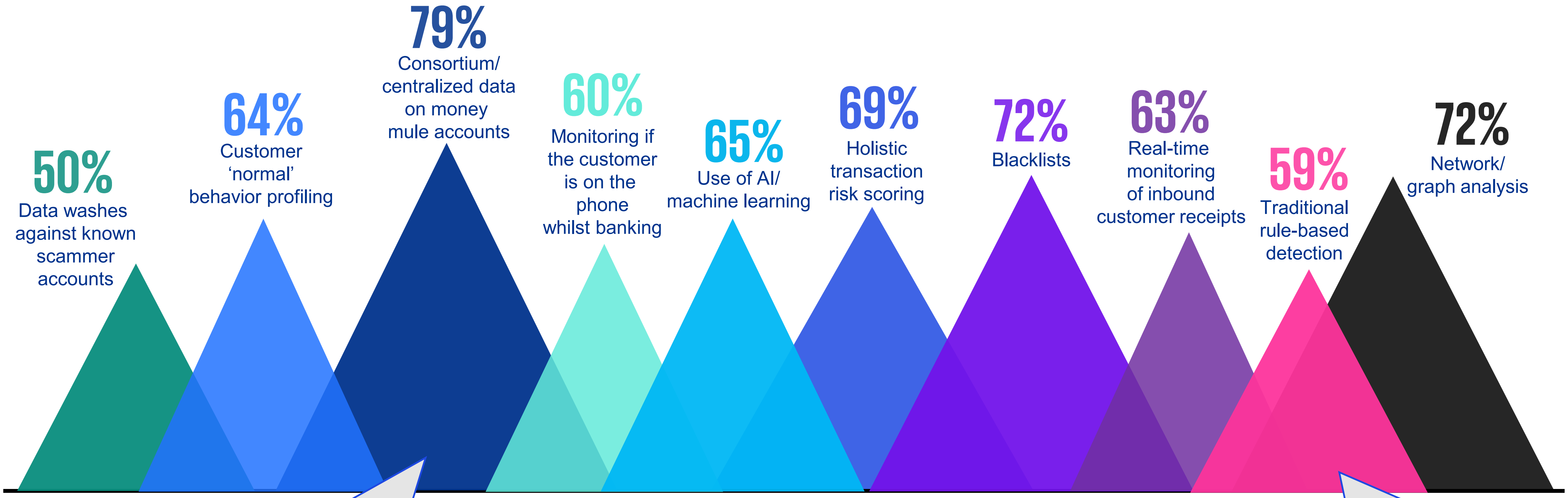
Targeted messaging with meaningful messages at the right time

Should be minimum standard in every market

## Some initiatives to protect vulnerable customers include:

- ❑ Customized monitoring rules
- ❑ Machine learning
- ❑ Recent scam victims identification
- ❑ Training
- ❑ Additional approval process
- ❑ Targeted education

# Effectiveness of detection methods



**Urgently required, said by countries without centralized data on mule accounts**

**This might not be useful in silo. Banks need to consider multiple factors.**

# Fraud responses

## How fraud operations teams investigated and resolved scam alerts

# Responsibilities of scam operations team

## Case management

Review cases, adhere regulatory and determine customer care pathway

## Investigations

Probe alerts and suspect mule accounts

## Customer communication

Act as a direct point of contact for the victims

## Asset tracing

Trace and recover customer funds

## Claims

Make decisions on claims in scam cases

## Trend spotting

Identify trends and new typologies to prevent future scams

# Duty of care for known scams

- Blocking transactions
- Informed consent
- Adding friction
- Risk profiles and proportionate responses
- Escalation and law enforcement
- Prioritizing customer choice

“ Banks **51%** elect to block transactions that could be mistakably linked to a scam”

# Protect your bank's reputation

**Strong brand protection ensures customer confidence, reinforces security measures and upholds the bank's reputation**

# Protect your bank's reputation

## Activities performed to protect the bank's reputation

- Dark web monitoring
- Impersonation
- Alpha tag protection
- Takedown services
- White hat hackers
- Do not originate lists

> “
> # Technology
> to prevent, detect and respond to APP scams needs to evolve as scams evolve”

## Next generation protection technology:

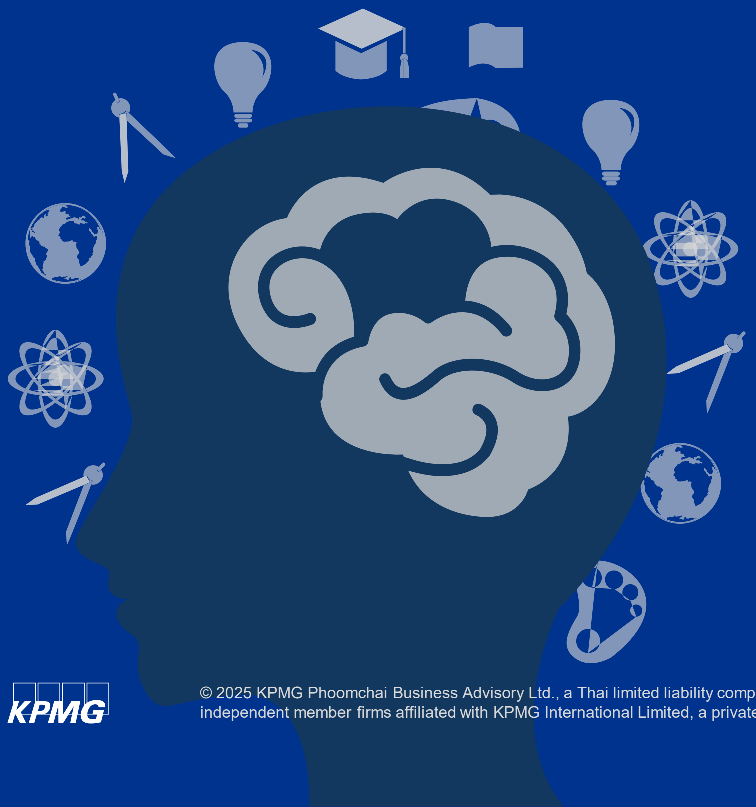
- Behavioral analytics
- Deepfake detection
- Dynamic and self-learning rule setting
- Dynamic warnings

**59%**

of respondents have an orchestration layer, while the others are currently building or implementing one.

# Customer education and awareness

> “Providing education about the signs and tactics of APP scams to customers helps them become better equipped to protect themselves”



## Which initiatives have you implemented?

95% Bank website guidance

90% Social media campaign

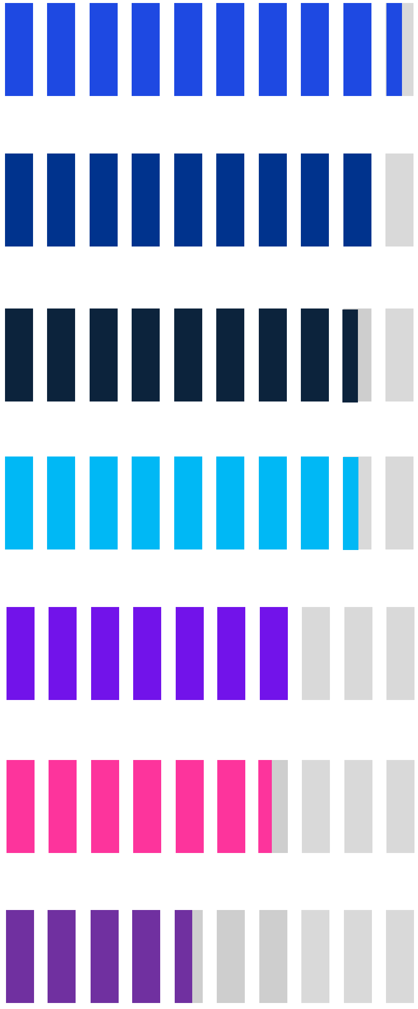
84% Collaborations with fraud prevention organizations

84% Scam alerts via emails or SMS

70% Educational webinars and workshops

63% TV or newspaper campaign

47% Interactive tools on website/mobile apps to help customers identify suspicious emails, websites or phone calls



# Challenges and Opportunities

Identified future challenges and opportunities in APP scam risk management

# Regulations

## Challenges

- The pace of regulatory changes is considered a significant challenge.
- Non-banks were perceived to be less accountable to regulatory requirements than banks in many jurisdictions.

## Opportunities

- Tailoring regulatory models from other countries to fit local contexts could ensure their effectiveness and relevance.
- Fostering collaboration across scam ecosystem will help industries combat APP scams.

# Data sharing

## Challenges

- Data privacy regulations may sometimes hinder the ability to share critical information, especially with cross-border transactions.

## Opportunities

- Transnational partnerships and consortium data modelling effectively combat fraud and money mule networks. It encompasses cross-sector data-sharing protocols and collaboration among banks, law enforcement, and other key ecosystem players.

# Technological advancements and AI

## Challenges

- Gen AI enables fraudsters to craft more sophisticated and convincing schemes, including bypassing basic customer identification measures.

## Opportunities

- Gen AI can help in scam risk management. For example, it could create tailored interactions to alert customers to specific risks.

# Customer awareness and education

## Challenges

- There was an acknowledgement of ‘message fatigue’ among customers. Banks need to think of new ways to deliver the messages.

## Opportunities

- There is an opportunity for government-funded campaigns to increase public awareness and empower customers to protect themselves with critical thinking and stronger authentication measures.

# Investment in technology and resources

## Challenges

- Continuous investment in new tools and training can keep banks with evolving scam techniques.
- The competition for skilled human resources and the migration of talent in some countries pose additional challenges.

## Opportunities

- Banks could consolidate anti-fraud operations and leverage machine learning to optimize fraud detection processes.

# Single view of the customer

## Challenges

- Some banks found it hard to have a fraud view of the customers across all channels and products, preventing them from proactively identifying scam behavior.

## Opportunities

- Banks are moving to consolidate data collection into an orchestration layer with GenAI-enabled teams to handle multiple functions.

# Key takeaways

Foster collaboration with regulators and industry partners to share insights, best practices and threat intelligence

Implement advanced fraud detection technologies to identify and mitigate fraudulent activities

Enhance cybersecurity measures to proactively detect and prevent banking scams

Establish a culture of vigilance and resilience within the organization to respond effectively to evolving scamming techniques

Prioritize customer education and awareness programs to empower individuals in recognizing and avoiding scamming tactics

**Nuttanich Chanitthikul**
**Director, Consulting – Enterprise Risk**

KPMG Phoomchai Business Advisory Ltd.
nuttanich@kpmg.co.th

**Chanikarn Srithundorn**
**Associate Director, Consulting – Enterprise Risk**

KPMG Phoomchai Business Advisory Ltd.
chanikarns@kpmg.co.th

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

**KPMG in Thailand**

**kpmg.com/th**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

**Document Classification: KPMG Public**